What is claimed is:

1. A method of processing first, second and third signals for use in a system having first, second, and third signal lines, comprising:

generating, using a pseudo-random number generator, pseudo-random output values; and

changing, as a function of at least one of said pseudo-random output values, which ones of the first, second, and third signal lines are used to transmit the first, second and third signals.

2. The method of claim 1, further comprising:

modifying at least one of the first, second or third signals, as a function of said one pseudo-random output value, prior to transmission of said one signal over one of said first, second, and third signal lines.

3. The method of claim 2, wherein the changing and modifying steps are performed by a matrix multiplication operation performed on the first, second, and third signals, the matrix multiplication operation utilizing matrix coefficients generated from a plurality of the pseudo-random output values.

4. The method of claim 3,

wherein the first, second, and third signal lines couple a source device to a destination device, said pseudo-random number generator contained within the source device, the method further comprising:

operating the source device to communicate with the destination device so as to establish a session key; and

operating the pseudo-random number generator to generate said pseudo-random output values as a function of the established session key.

5. The method of claim 4, wherein the first, second, and third signals correspond to color signals representing an image, the method further comprising:

utilizing a different session key for each line of an image that is transmitted.

6. The method of claim 5, wherein session key information is transmitted to the destination device during a video blanking period.

7. The method of claim 4, wherein the destination device includes an additional pseudo-random number generator, the method further comprising:

operating the destination device to perform, as a function of an output of the additional pseudo-random number generator, the inverse of the changing and modifying steps performed by the source device to restore the first, second and third signals to their original condition so as to yield restored first, second and third signals.

8. The method of claim 7, wherein the first, second and third signals are analog red, green and blue color video signals, respectively, the source device is a computer

system display adapter, and the destination device is a computer monitor; the method further comprising:

displaying, on a display screen included in the destination device, an image represented by restored first, second and third color video signals.

9. The method of claim 1, wherein the first, second and third signal lines couple a source device to a destination device, said pseudo-random number generator being included in the source device, the method further comprising:

operating the source device to communicate with the destination device to establish a session key; and

operating the pseudo-random number generator to generate said pseudo-random output values as a function of the established session key.

10. The method of claim 9, wherein the method further comprises, prior to establishing a session key:

operating the source device to request identification information from the destination device; and

if the identification information is received from the display device, determining from the identification information, if the destination device is an encryption capable device.

11. The method of claim 10, further comprising:

if no identification information is received in a preselected period of time after requesting

identification information, restricting the output of the source device over the first, second and third lines to unencrypted video signals which are not subject to restrictions prohibiting their transmission in unencrypted form over analog transmission lines, the unencrypted video signals being fourth, fifth and sixth video signals.

12. The method of claim 10, wherein the identification information received from the destination device includes a digital certificate confirming identify of the destination device if the destination device is an encryption capable device; and wherein determining if the destination device is an encryption capable device includes the act of checking the received identification information to determine if said received identification information includes said digital certificate.

13. The method of claim 11, wherein the source device is a display adapter, the method further comprising:

storing session keys used to encrypt video data on the display adapter; and

limiting export of video data subject to copy constraints to video data that is in encrypted form.

14. The method of claim 13, further comprising:

interfacing with electronics devices though a 1394 interface.

15. A method of generating encrypted analog first, second and third signals (R', G', B', respectively) from

first, second, and third analog input signals (R, G, B, respectively) the method comprising:

pseudo-randomly generating at least one of a plurality of matrix coefficients, a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3;

using an encryption circuit to perform a matrix multiplication operation to generate the encrypted analog first, second, and third signals, according to the following equations:

$$R' = a_1R + b_1G + c_1B$$
$$G' = a_2R + b_2G + c_2B$$
$$B' = a_3R + b_3G + c_3B.$$

16. The method of claim 15, wherein the matrix coefficients are generated such that the set of matrix coefficients a_1, b_1, c_1 include two values which are the same and one value that is different.

17. The method of claim 16, wherein the matrix coefficients are further generated such that:

the set of matrix coefficients a_2, b_2, c_2 include two values which are the same and one value that is different; and

the set of matrix coefficients a_3, b_3, c_3 include two values which are the same and one value that is different.

18. The method of claim 17, wherein the matrix coefficients are further generated such that:

the set of matrix coefficients a_1, a_2, a_3 include two values which are the same and one value that is different;

the set of matrix coefficients b_1, b_2, b_3 include two values which are the same and one value that is different; and.

the set of matrix coefficients c_1, c_2, c_3 include two values which are the same and one value that is different.

19. The method of claim 16, wherein the two values which are the same are positive values and the value which is different is a negative value.

Sub A1

20. The method of claim 15, wherein the matrix coefficients are generated such that each of the R', G' and B' signals will be the product of summing two signals in the set of analog signals R, G, B and subtracting one of the signals in the set of analog signals R, G, B.

21. The method of claim 15, wherein the matrix multiplication operation includes the acts of:

performing analog multiplication operations to multiply the R, G, and B signals by the coefficients a_1, b_1, c_1, respectively.

22. The method of claim 15, wherein the first, second and third signals correspond to red, green and blue video signals, respectively.

23. The method of claim 22 performed by a source device and further comprising:

communicating with a destination device to establish a content encryption key to be used as an input to the pseudo-random number generator.

24. The method of claim 23, further comprising:

using a different content encryption key when encrypting portions of the first, second and third video signals which correspond to different lines of an image.

25. A communication method comprising the steps of:

using a pseudo-random number generator to generate output values; and

modifying first, second and third signals, by performing a matrix multiplication operation thereon utilizing matrix coefficients which are a function of at least one of the pseudo-random output values, the modified first, second and third signals being encrypted analog signals so as to define first, second and third encrypted analog signals; and

transmitting the first, second and third encrypted analog signals to a destination device.

26. The method of claim 19, wherein the matrix coefficients correspond to a 3x3 array of matrix coefficients, each row of coefficients including two coefficients of the same value and one coefficient of a different value.

27. The method of claim 26, wherein the two coefficients of the same value are positive valued coefficients and the one coefficient of a different value is a negative value coefficient.

28. The method of claim 25, wherein the matrix multiplication operation includes the act of:

performing a plurality of analog signal multiplication operations.

29. The method of claim 28, wherein the matrix multiplication operation further includes the act of:

performing a plurality of analog signal addition operations.

Sub A1

30. The method of claim 25, wherein said matrix multiplication involves summing an integer multiple of two of the first, second and third signals and subtracting an integer multiple of another one of said first second and third signals to produce the first encrypted analog signal.

31. The method of claim 25, further comprising:

establishing an encryption key with the destination device; and

using the encryption key as an input to the pseudo-random number generator, said one pseudo-random output value being generated as a function of the encryption key.

32. The method of claim 31, further comprising:

operating the destination device to decrypt the first, second and third encrypted analog signals utilizing the encryption key.

33. The method of claim 32, wherein operating the destination device to decrypt the first, second and third encrypted analog signals comprises the act of performing a matrix multiplication operation on the first, second and third encrypted analog signals utilizing matrix coefficients generated from said at least one pseudo-random output value.

34. The method of claim 33, wherein the source device is a display adapter, the destination device is a display device, and the first, second and third signals are red, green and blue video signals, respectively.

35. A computer readable medium comprising:

computer executable instructions for controlling a computer device to perform the steps of:

operating a pseudo-random number generator to generate a pseudo-random output value; and

modifying first, second and third signals, by performing a matrix multiplication operation thereon utilizing matrix coefficients at least one of which is a function of the pseudo-random number output value so as to define first, second and third encrypted analog signals; and

transmitting the first, second and third encrypted analog signals to a destination device.

36. A device, comprising:

a video signal encryption circuit for encrypting, in response to a pseudo-random number, red, green and blue video signals and for producing first, second and third analog encrypted video signals;

a pseudo-random number generator circuit, coupled to the video signal encryption circuit, for producing the pseudo-random number value; and

an input/output interface for outputting the first, second and third encrypted analog video signals.

37. The device of claim 36, further comprising means for communicating with a destination device for establishing a session key to be used for encrypting and decrypting the red, green and blue analog encrypted video signals.

38. The device of claim 36, further comprising,

video processor circuitry for processing received video signals;

an additional input/output interface for coupling the video processor to a system bus and a IEEE 1394 compliant bus; and

a content cipher subsystem for encrypting and decrypting information communicated over the IEEE 1394 compliant bus.

39. The device of claim 36, further comprising:

a physically secure non-volatile memory device for storing encryption keys; and

means for limiting export from the device of video data, subject to copy restrictions, received in encrypted

form over the IEEE 1394 bus to video data that is in an encrypted form.

40. The device of claim 39, wherein the video signal encryption circuit comprises a matrix multiplier for performing a matrix multiplication operation on the red, green and blue video signals.

41. A method of decrypting encrypted analog signals including the steps of:

generating a first decrypted analog signal from a first pair of encrypted analog signals by:

summing the two encrypted analog signals in the first pair of analog signals to produce a first sum; and

dividing the first sum by a first value to produce a first decrypted analog signal.

42. The method of claim 41, further comprising:

generating a second decrypted analog signal from a second pair of encrypted analog signals by:

summing the two encrypted analog signals in the second pair of analog signals to produce a second sum; and

dividing the second sum by a second value to produce a second decrypted analog signal.

43. The method of claim 42, further comprising:

generating a third decrypted analog signal from a third pair of encrypted analog signals by:

summing the two encrypted analog signals in the third pair of analog signals to produce a third sum; and

dividing the third sum by a third value to produce a third decrypted analog signal.

44. The method of claim 43, wherein the first, second and third values are the same.

45. The method of claim 44, wherein the first, second and third values are integer multiples of 2.

46. The method of claim 44, further comprising the step of:

periodically changing the value used for the first, second and third values as a function of the output of a pseudo random number generator.

47. The method of claim 41, further comprising:

comparing values in first and second rows of values to identify a first column of values in which the first and second rows of values include the same value; and

controlling which one of a plurality of output lines the first decrypted analog signal is transmitted on as a function of the identified column of values.

48. The method of claim 43, further comprising:

comparing values in first and second rows of values to identify a first column in which the first and second rows of values include the same value;

comparing values in second and third rows of values to identify a second column in which the second and third rows of values include the same value, the second column being different than said first column;

and

controlling which one of a plurality of output lines the first decrypted analog signal is transmitted on as a function of the identified first column and which one of the plurality of output lines the second decrypted analog signal is transmitted on as a function of the identified second column, the first and second decrypted analog signals being transmitted on different output lines.

49. The method of claim 48, wherein the first and second rows of values are first and second rows of values included in a permutation matrix used to encrypt the analog signals included in the first pair of signals.

50. The method of claim 48, further comprising:

comparing values in a third row of values and said first row of values to identify a third column in which the third and first rows of values include the same value;

and

controlling which one of a plurality of output lines the third decrypted analog signal is transmitted on as a function of the identified third column, the third

decrypted analog signal being transmitted on a different output line from said first and second decrypted analog signals.

51. The method of claim 49, wherein the first and second rows of values are first and second rows of values included in a permutation matrix used to encrypt the analog signals included in the first pair of signals;

wherein the second and third rows of values are second and third rows of values included in said permutation matrix; and

.wherein the third and first rows of values are third and first rows of values included in said permutation matrix.

52. The method of claim 48,

wherein the first, second and third decrypted analog signals are red, green and blue analog video signals; and

wherein the plurality of output lines include red, green and blue output lines which are coupled to a display device.

53. A method of generating an encrypted analog signal from at least two of a first analog input signal, a second analog input signal, and a third analog input signal, the method comprising:

pseudo-randomly generating an encryption value;

multiplying a first one of said first, second, and third analog input signals with said encryption value to produce a multiplied signal; and

combining said multiplied signal with at least a second signal generated from a second one of said first, second, and third analog input signals to produce said encrypted analog signal.

54. The method of claim 53, wherein said multiplying and said combining are performed as part of a matrix multiplication operation.

A1

55. The method of claim 53, wherein said encryption value is a matrix coefficient and wherein said matrix multiplication operation is performed using analog multipliers.